

# STATISTICS FOR BIQUADRATIC COVERS OF THE PROJECTIVE LINE OVER FINITE FIELDS.

ELISA LORENZO, GIULIO MELELEO, AND PIERMARCO MILIONE  
WITH AN APPENDIX BY ALINA BUCUR

**ABSTRACT.** We study the distribution of the traces of the Frobenius endomorphism of genus  $g$  curves which are quartic non-cyclic covers of  $\mathbb{P}_{\mathbb{F}_q}^1$ , as the curve varies in an irreducible component of the moduli space. We show that for  $q$  fixed, the limiting distribution of the trace of Frobenius equals the sum of  $q + 1$  independent random discrete variables. We also show that when both  $g$  and  $q$  go to infinity, the normalized trace has a standard complex Gaussian distribution. Finally, we extend these computations to the general case of arbitrary covers of  $\mathbb{P}_{\mathbb{F}_q}^1$  with Galois group isomorphic to  $r$  copies of  $\mathbb{Z}/2\mathbb{Z}$ . For  $r = 1$ , we recover the already known hyperelliptic case.

## 1. INTRODUCTION

One of the most influent result in class field theory is Chebotarev's density theorem. As it is well known, this result is a deep generalization of the Theorem of Dirichlet about equidistribution of rational primes in arithmetic progression and gives a complete understanding of the distribution of primes in a fixed Galois number field extension with respect to their splitting behavior (for an interesting discussion of the theorem and its original proof see [LS96]). In the function field case, the parallel statement is carried over by the Sato-Tate conjecture for curves, which studies the distribution of the Frobenius endomorphism of the reduction modulo  $p$  of a fixed curve, when the prime  $p$  varies.

In order to complement this research line in other directions, several mathematicians were led to consider the following new general problem: given a family of curves, of genus  $g$  over  $\mathbb{F}_q$ , satisfying certain properties, understand the distribution of the Frobenius endomorphism of the curves of the family. This is sometimes called the *vertical Sato-Tate conjecture*, since the prime  $p$  is fixed and the curve varies in the family. We can study the limiting distribution in two different ways, depending on whether we let the genus  $g$  or the cardinality  $q$  of the field tend to infinity. It is then interesting to compare both limit results.

When  $g$  is fixed and  $q$  goes to infinity the problem can be solved thanks to Deligne's equidistribution theorem (cf. [KS99]) while for the complementary case different techniques are applied depending on the particular family considered. The fluctuation in the number of points at the  $g$ -limit has been studied for different families of curves, such as:

- Hyperelliptic curves, cf. [KR09], [BDFL09],
- Cyclic trigonal curves (i.e. cyclic 3-covers of the projective line), cf. [BDFL09], [Xio10],
- General trigonal curves, cf. [Woo12],
- $p$ -fold cover of the projective line, [BDFL11],
- $\ell$ -covers of the projective line, cf. [BDFL09], [BDF<sup>+</sup>15].

---

2010 *Mathematics Subject Classification.* 11G20, 14H05, 11M50.

*Key words and phrases.* Function fields, biquadratic curves, biquadratic covers, number of points over finite fields, arithmetic statistics.

The second author was partially supported by the "National Group for Algebraic and Geometric Structures, and their Applications" (GNSAGA-INDAM). The third author was partially supported by the Spanish Council under project MTM2012-33830 and by an ADR grant from the Universitat de Barcelona.

In the present paper, we study the distribution of the number of points over  $\mathbb{F}_q$  for a genus  $g$  curve  $C$  defined over  $\mathbb{F}_q$  which is a quartic non-cyclic cover of the projective line  $\mathbb{P}_{\mathbb{F}_q}^1$ , at the  $q$ -limit (for a genus  $g$  fixed) and at the  $g$ -limit (with  $q$  fixed). This is the first time that a family of non-cyclic abelian covers is studied. The distribution obtained is different to the product of probabilities for the family of hyperelliptic curves, what at first sight could be guessed. Therefore, the study of this family seems to be the first natural step in order to understand the general abelian case.

Let  $\mathcal{B}_g(\mathbb{F}_q)$  be the family of genus  $g$  quartic non-cyclic cover of the projective line  $\mathbb{P}_{\mathbb{F}_q}^1$ , and consider the following decomposition

$$\mathcal{B}_g(\mathbb{F}_q) = \bigcup_{g_1+g_2+g_3=g} \mathcal{B}_{(g_1,g_2,g_3)}(\mathbb{F}_q)$$

where  $\mathcal{B}_{(g_1,g_2,g_3)}(\mathbb{F}_q)$  denotes the subfamily of curves  $C \in \mathcal{B}_g(\mathbb{F}_q)$  such that the three hyperelliptic quotients of  $C$  have genera  $g_1, g_2$  and  $g_3$ .

The main theorem of the paper is the following:

**Theorem 4.1** *If the three genera  $g_1, g_2, g_3$  go to infinity, then we have that*

$$\frac{|\{C \in \mathcal{B}_{(g_1,g_2,g_3)}(\mathbb{F}_q) : \text{Tr}(\text{Frob}_C) = -M\}|}{|\mathcal{B}_{(g_1,g_2,g_3)}(\mathbb{F}_q)|} = \text{Prob} \left( \sum_{j=1}^{q+1} X_j = M \right)$$

where the  $X_j$  are i.i.d. (identically independently distributed) random variables such that

$$X_i = \begin{cases} -1 & \text{with probability } \frac{3(q+2)}{4(q+3)} \\ 1 & \text{with probability } \frac{6}{4(q+3)} \\ 3 & \text{with probability } \frac{q}{4(q+3)} \end{cases}.$$

**Outline.** In Section 2, we introduce the family of biquadratic curves and we give a parametrization of the family in terms of coprime square-free polynomials. In Section 3, we compute the monodromy group of the family in the sense of Katz and Sarnak (cf. [KS99, Ch. 9]) and we obtain the corresponding distribution of the Frobenius traces at the  $q$ -limit. In Section 4, previous theorem is proven, and in Section 5 the moments of the Frobenius traces are computed at the  $g$ -limit, proving that when both  $g$  and  $q$  go to infinity the normalized trace has a standard complex Gaussian distribution. In last section, Theorem 4.1 is generalized for an arbitrary cover of the projective line with Galois group isomorphic to  $r$  copies of  $\mathbb{Z}/2\mathbb{Z}$ . The paper concludes with an Appendix, written by Alina Bucur, giving the heuristic for the distribution of the number of points for the whole family of  $r$ -quadratic curves.

**Notations.** We now fix some notations and conventions that will be valid in the sequel.

- $p \neq 2$  is a prime integer, and  $q$  is a positive power of  $p$ .
- $k = \mathbb{F}_q(t)$  is the function field of  $\mathbb{P}_{\mathbb{F}_q}^1$ , and  $K/k$  is a finite extension.
- $(f, g)$  denotes the greatest common divisor of two polynomials  $f, g \in \mathbb{F}_q[t]$ .
- $\deg(f)$  denotes the degree of a polynomial  $f$ .
- $|f| := q^{\deg(f)}$  denotes the norm of a polynomial  $f$ .
- $\check{f}$  is the polynomial obtained inverting the order of the coefficients of  $f$ .
- $g(C)$  denotes the geometric genus of the projective curve  $C/\mathbb{F}_q$ ,
- and  $\text{Frob}_C$  denotes its geometric Frobenius morphism.

**Acknowledgements.** This work was started in March 2014 at the Arizona Winter School “Arithmetic Statistic” and the authors would like to thank the organizers for creating such a stimulating working environment. Moreover, the authors are grateful to Alina Bucur and Chantal David for initiating them into this rich and appealing field of research in number theory and for several discussions and helpful comments during the preparation of the paper. Finally, we would like to thank Patrick Meisner for carefully reading a first draft of the paper and for his useful comments.

## 2. THE FAMILY OF BIQUADRATIC CURVES

We first define and give the basic properties of the family of biquadratic curves. We determine its genus in terms of the equations defining the curves, and we study the irreducible components of the coarse moduli space of biquadratic curves.

Recall that if  $K/\mathbb{F}_q(t)$  is a finite Galois extension such that  $K \cap \bar{\mathbb{F}}_q = \mathbb{F}_q$ , then there exists, up to isomorphism, a unique nonsingular projective curve  $C$  with function field  $\mathbb{F}_q(C) = K$ , together with a regular morphism  $\varphi : C \rightarrow \mathbb{P}_{\mathbb{F}_q}^1$  defined over  $\mathbb{F}_q$  (cf. [Har77, I, Th. 6.6, Th.6.9]).

**Definition 2.1.** *We call biquadratic curve a smooth projective curve  $C$ , together with a regular morphism  $\varphi : C \rightarrow \mathbb{P}_{\mathbb{F}_q}^1$  defined over  $\mathbb{F}_q$ , that induces a field extension with Galois group  $\text{Gal}(\mathbb{F}_q(C)/\mathbb{F}_q(t)) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .*

Since  $\text{char}(k) \neq 2$ , it is clear that every non-cyclic quartic extension of  $k$  is of the form  $K = k(\sqrt{h_1(t)}, \sqrt{h_2(t)})$ , for some  $h_1(t), h_2(t) \in \mathbb{F}_q[t]$  different non-constant polynomials, that we can take to be square-free. Moreover, if the leading coefficient of  $h_i$  is a square in  $\mathbb{F}_q$ , then we can assume that this is equal to 1. Therefore, if  $C$  is a biquadratic curve, then an affine model of  $C$  in  $\mathbb{A}_{\mathbb{F}_q}^3$  is given by

$$C : \begin{cases} y_1^2 = h_1(t) \\ y_2^2 = h_2(t) \end{cases}.$$

**Remark 2.2.** If  $K := k(\sqrt{h_1(t)}, \sqrt{h_2(t)})$  is a biquadratic extension of  $k$ , then there are exactly 3 different quadratic subextensions of  $K$ , namely  $k(\sqrt{h_1})$ ,  $k(\sqrt{h_2})$  and  $k(\sqrt{h_1 h_2})$ .

If we write  $h_i = f_i f$  for  $i = 1, 2$ , with  $f = (h_1, h_2)$ , then clearly we have that  $(f_1, f_2) = (f_1, f) = (f_2, f) = 1$  and these three subextensions are  $k(\sqrt{f f_1})$ ,  $k(\sqrt{f f_2})$  and  $k(\sqrt{f_1 f_2})$ .

Two such extensions  $k(\sqrt{h_1(t)}, \sqrt{h_2(t)})$  and  $k(\sqrt{h'_1(t)}, \sqrt{h'_2(t)})$  define the same biquadratic extension if and only if we have the equality of sets

$$\{h_1, h_2, \frac{h_1 h_2}{(h_1, h_2)^2}\} = \{h'_1, h'_2, \frac{h'_1 h'_2}{(h'_1, h'_2)^2}\}.$$

**Remark 2.3.** Recall that if  $\pi : C \rightarrow \mathbb{P}^1$  is a degree 2 regular cover, whose affine plane model is  $y^2 = F(t)$ , with  $F(t)$  a square-free polynomial over  $\mathbb{F}_q$ , then the point at infinity is ramified in the cover  $\pi$  if and only if the degree  $d$  of  $F$  is odd. Indeed, if we take  $u = \frac{1}{t}$ , then the function field of  $C$  is

$$k(C) = k(\sqrt{F(t)}) = k(\sqrt{F(1/u)}) = k(\sqrt{u^{-d} \tilde{F}(u)})$$

and then it is clear that  $t = \infty$  ramifies if and only if the point  $u = 0$  ramifies, i.e. if and only if  $d$  is odd.

**Proposition 2.4.** *Let  $h_1(t), h_2(t) \in \mathbb{F}_q[t]$  be different square-free polynomials, and let  $C$  be the curve whose function field is  $k(C) = k(\sqrt{h_1(t)}, \sqrt{h_2(t)})$ . For every  $i = 1, 2$ , write  $h_i = f f_i$ , with  $f = (h_1, h_2)$ , and define  $h_3 := f_1 f_2$ .*

If we denote by  $C_i$  the hyperelliptic curve whose affine plane model is given by the equations  $y^2 = h_i(t)$ , for  $i = 1, 2, 3$ , then we have the following formula for the genus of  $C$ :

$$g(C) = g(C_1) + g(C_2) + g(C_3).$$

Moreover, if we denote by  $n := \deg(f)$  and  $n_i := \deg(f_i)$ ,

$$g(C) = g(n_1, n_2, n) := n_1 + n_2 + n + e_\infty - 4,$$

where  $e_\infty$  is the ramification index at the point at infinity, that is,

$$e_\infty := \begin{cases} 2, & \text{if } n \equiv n_1 \equiv n_2 \equiv 0 \pmod{2} \\ 1, & \text{otherwise} \end{cases}.$$

*Proof.* Let us denote by  $R := \text{Ram}(\pi)$  the subset of all points of  $\mathbb{P}_{\mathbb{F}_q}^1$  which are ramified in the cover  $\pi : C \rightarrow \mathbb{P}_{\mathbb{F}_q}^1$ . Riemann-Hurwitz's formula (cf. [Ros02, Theorem 7.16]) implies that  $2g(C) - 2 = 4(2 \cdot 0 - 2) + 2|R|$ . That is,  $g(C) = |R| - 3$ . Again, for the hyperelliptic cover  $\pi_i : C_i \rightarrow \mathbb{P}^1$  and the ramification sets  $R_i := \text{Ram}(\pi_i)$ , we get  $g(C_i) = \frac{|R_i|}{2} - 1$ . Now, the definition of  $h_3$  implies that

$$2|R_1 \cup R_2 \cup R_3| = |R_1| + |R_2| + |R_3|.$$

Thus, the formula  $g(C) = g(C_1) + g(C_2) + g(C_3)$  holds.

We can also apply Riemann-Hurwitz's formula to the morphism  $\pi$ , and so we have

$$2g - 2 = 4(2 \cdot 0 - 2) + 2 \cdot (n_1 + n_2 + n_3 + e_\infty - 1).$$

□

Now, we introduce some sets of polynomials that will be useful:

$$\begin{aligned} V_d &= \{F \in \mathbb{F}_q[t] : F \text{ monic, } \deg(F) = d\}, \\ \mathcal{F}_d &= \{F \in \mathbb{F}_q[t] : F \text{ monic, square-free, } \deg(F) = d\}, \\ \widehat{\mathcal{F}}_d &= \{F \in \mathbb{F}_q[t] : F \text{ square-free, } \deg(F) = d\}, \\ \mathcal{F}_{(n, n_1, n_2)} &= \{(f, f_1, f_2) \in \mathcal{F}_n \times \mathcal{F}_{n_1} \times \mathcal{F}_{n_2} : (f, f_1) = (f, f_2) = (f_1, f_2) = 1\}, \\ \widehat{\mathcal{F}}_{(n, n_1, n_2)} &= \{(f, f_1, f_2) \in \mathcal{F}_n \times \widehat{\mathcal{F}}_{n_1} \times \widehat{\mathcal{F}}_{n_2} : (f, f_1) = (f, f_2) = (f_1, f_2) = 1\}, \\ \mathcal{F}_{[n, n_1, n_2]} &= \mathcal{F}_{(n, n_1, n_2)} \cup \mathcal{F}_{(n-1, n_1, n_2)} \cup \mathcal{F}_{(n, n_1-1, n_2)} \cup \mathcal{F}_{(n, n_1, n_2-1)}, \\ \widehat{\mathcal{F}}_{[n, n_1, n_2]} &= \widehat{\mathcal{F}}_{(n, n_1, n_2)} \cup \widehat{\mathcal{F}}_{(n-1, n_1, n_2)} \cup \widehat{\mathcal{F}}_{(n, n_1-1, n_2)} \cup \widehat{\mathcal{F}}_{(n, n_1, n_2-1)}. \end{aligned}$$

**Definition 2.5.** We denote by  $\mathcal{B}_g(\mathbb{F}_q)$  the family of biquadratic curves defined over  $\mathbb{F}_q$  and of fixed genus  $g$ . It can be written as a disjoint union of subfamilies indexed by unordered 3-tuples of positive integers  $g_1, g_2, g_3$ , i.e.

$$\mathcal{B}_g(\mathbb{F}_q) = \bigcup_{g_1+g_2+g_3=g} \mathcal{B}_{(g_1, g_2, g_3)}(\mathbb{F}_q),$$

where  $\mathcal{B}_{(g_1, g_2, g_3)}(\mathbb{F}_q)$  denotes the subfamily of biquadratic curves of genus  $g = g_1 + g_2 + g_3$  such that the intermediate curves given by the morphism to  $\mathbb{P}^1$  have genus equal to  $g_1, g_2$  and  $g_3$ . This family is in bijection with the family of curves defined by elements in the set of polynomials  $\widehat{\mathcal{F}}_{[n, n_1, n_2]}$  such that  $g_i = \lfloor \frac{n+n_i-1}{2} \rfloor$  for  $i = 1, 2$  and  $g_3 = \lfloor \frac{n_1+n_2-1}{2} \rfloor$ .

The family  $\mathcal{B}_g(\bar{\mathbb{F}}_q)$  of biquadratic curves defined over  $\bar{\mathbb{F}}_q$  is a coarse moduli space over  $\mathbb{Z}[1/2]$  (cf. [GP05b, Lemma 3.1]). A detailed geometric study of this moduli space can be found in [GP05b] and [GP05a].

**Remark 2.6.** One has the following equalities:

$$|\mathcal{B}_{(g_1, g_2, g_3)}(\mathbb{F}_q)|' = \sum_{C \in \mathcal{B}_{(g_1, g_2, g_3)}(\mathbb{F}_q)} 1 = \sum_{F \in \widehat{\mathcal{F}}_{[n, n_1, n_2]}} \frac{1}{|\text{Aut}(C)|} = \frac{|\widehat{\mathcal{F}}_{[n, n_1, n_2]}|}{q(q^2 - 1)},$$

where the  $'$  notation, applied both to cardinality and summation, means that each one of the curves  $C$  in the moduli spaces is counted with the usual weight  $\frac{1}{|\text{Aut}(C)|}$ .

**Remark 2.7.** Notice that  $|\widehat{\mathcal{F}}_{(n, n_1, n_2)}| = (q - 1)^2 |\mathcal{F}_{(n, n_1, n_2)}|$  and that we can see the set  $\widehat{\mathcal{F}}_{(n, n_1, n_2)}$  as the set of the quadratic twists of elements in  $\mathcal{F}_{(n, n_1, n_2)}$  given by the equations

$$C' : \begin{cases} y_1^2 = \alpha_1 f f_1(t) \\ y_2^2 = \alpha_2 f f_2(t) \end{cases}$$

where  $\alpha_1, \alpha_2 \in \mathbb{F}_q^*$ .

### 3. MONODROMY GROUP OF THE FAMILY

A useful reference for this section is [KS99, Ch. 9]. Let  $S$  be an open set of  $\text{Spec } \mathbb{F}_q$  and let  $\mathcal{C} \rightarrow S$  be a smooth proper morphism of schemes such that the geometric fibers  $C_x \otimes \overline{\mathbb{F}}_q$  are smooth projective curves of genus  $g$  over  $\overline{\mathbb{F}}_q$ .

Fix a prime integer  $\ell \neq p$ . Then, there exists an  $\ell$ -adic representation

$$\rho_\ell : \pi_1(S) \longrightarrow \text{GL}_{2g}(\overline{\mathbb{Q}}_\ell)$$

with the following interpolation property: for every closed point  $x : \text{Spec } \mathbb{F}_q \rightarrow S$  the induced representation

$$\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \simeq \pi_1(\text{Spec } \mathbb{F}_q) \longrightarrow \pi_1(S) \longrightarrow \text{GL}_{2g}(\overline{\mathbb{Q}}_\ell)$$

is isomorphic to the  $\ell$ -adic representation

$$\rho_{C_x, \ell} : \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \longrightarrow \text{Aut}(H_{\text{et}}^1(C_x \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q, \overline{\mathbb{Q}}_\ell)) \simeq \text{GL}_{2g}(\overline{\mathbb{Q}}_\ell).$$

Once an embedding  $\iota : \overline{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C}$  is fixed, we have a  $2g$ -dimensional complex representation  $\iota \cdot \rho_\ell$ . The image of this representation is a subgroup of  $\text{GL}_{2g}(\mathbb{C})$  called the monodromy group of the family.

For every integer  $d \geq 1$ , the set of polynomials  $\mathcal{F}_d$  defined in Section 2 can be algebraically realized as a Zariski-open subset of  $\mathbb{A}_{\mathbb{F}_q}^d$ . This could be done redefining it in the following way:

$$\mathcal{F}_d := \{(a_0, \dots, a_{d-1}) \in \mathbb{A}_{\mathbb{F}_q}^d \mid D(a_0, \dots, a_{d-1}) \neq 0\},$$

where  $D : \mathbb{A}_{\mathbb{F}_q}^d \rightarrow \mathbb{A}_{\mathbb{F}_q}^1$  is the continuous function such that  $D(a_0, a_1, \dots, a_{d-1})$  denotes the discriminant of the monic polynomial  $a_0 + a_1 t + \dots + t^d \in \mathbb{F}_q[t]$ .

Let  $\mathcal{H}_g$  denote the family of genus  $g$  hyperelliptic curves over  $\mathcal{F}_d$ , whose fiber over the polynomial  $F \in \mathcal{F}_d$  is given by the curve whose affine plane model is  $y^2 = F(t)$ . In [KS99, 10.1], it is proved that the monodromy group either of the family  $\mathcal{H}_g$  over  $\mathcal{F}_{2g+1}$  and of the family  $\mathcal{H}_g$  over  $\mathcal{F}_{2g+2}$  is  $G_{\text{geom}} = \text{Sp}_{2g}(\mathbb{C})$ .

**Proposition 3.1.** *The monodromy group of the family  $\mathcal{B}_{g_1, g_2, g_3}(\mathbb{F}_q)$  is the biggest possible one, namely it is the symplectic group  $\text{Sp}_{2g}(\mathbb{C})$ .*

*Proof.* The set of polynomials  $\mathcal{F}_{[n, n_1, n_2]}$  defined in Section 2 can be realized as a Zariski-open subset of  $\mathbb{A}_{\mathbb{F}_q}^n \times \mathbb{A}_{\mathbb{F}_q}^{n_1+1} \times \mathbb{A}_{\mathbb{F}_q}^{n_2+1}$ .

The family of genus  $g$  curves over  $\mathcal{F}_{[n,n_1,n_2]}$ , whose fiber over the 3-tuple  $(f, f_1, f_2) \in \mathcal{F}_{[n,n_1,n_2]}$  is given by the curve whose affine model is  $y_1^2 = f f_1(t), y_2^2 = f f_2(t)$ , is exactly the subfamily of genus  $g$  biquadratic curves  $\mathcal{B}_{g_1,g_2,g_3}(\mathbb{F}_q)$  defined in Section 2.

Let  $N := \max(n, n_2, n_3)$ . By the symmetry of the parametrization we can assume for example that  $N = n$  and then we fix two square-free polynomials  $f_1, f_2$  of degrees  $n_1, n_2$  such that  $f_1 f_2$  is also square-free. Therefore, we can consider the open immersion

$$\{f \in \mathcal{F}_n : f f_1, f f_2 \text{ square-free}\} \longrightarrow \mathcal{F}_{[n,n_1,n_2]} : f \longmapsto (f, f_1, f_2).$$

The monodromy group of the family  $\mathcal{H}_g$  of hyperelliptic curves over this subset of  $\mathcal{F}_n$  is the same as if we consider the family over all  $\mathcal{F}_n$ . Finally, the monodromy group of the family  $\mathcal{B}_{(g_1,g_2,g_3)}(\mathbb{F}_q)$  can only increase and, after results of [KS99, 10.1], it is the biggest possible one.  $\square$

Applying Deligne's equidistribution theorem (cf. [KS99, 9.3,9.2]) and random matrix theory (cf. [DS94, 4]), we have the following distribution result at the  $q$ -limit for the family  $\mathcal{B}_{(g_1,g_2,g_3)}(\mathbb{F}_q)$ .

**Corollary 3.2.** *Let  $g \geq 3$  be a fixed integer. When  $q$  goes to  $\infty$ , the classes of the Frobenius automorphisms  $\{\text{Frob}_C\}_{C \in \mathcal{B}_{(g_1,g_2,g_3)}(\mathbb{F}_q)}$  acting on the first étale cohomology group  $H_{\text{ét}}^1(C, \mathbb{Q}_\ell)$  are equidistributed with respect to the Haar measure associated to the maximal compact subgroup of  $\text{Sp}_{2g}(\mathbb{C})$ , i.e.*

$$\lim_{q \rightarrow \infty} \langle \text{Tr Frob}_C^m \rangle = \begin{cases} 2g & m = 0 \\ -\eta_r & 1 \leq |m| \leq 2g \\ 0 & |m| > 2g \end{cases}$$

where

$$\eta_m := \begin{cases} 1 & m \text{ even} \\ 0 & m \text{ odd} \end{cases}.$$

#### 4. THE NUMBER OF POINTS OVER $\mathbb{F}_q$

Let  $\chi$  denote the quadratic character in  $\mathbb{F}_q$ . We set, for any element  $(f, f_1, f_2)$  in  $\widehat{\mathcal{F}}_{(n,n_1,n_2)}$ ,

$$S(f, f_1, f_2) = \sum_{x \in \mathbb{F}_q} (\chi(f \cdot f_1(x)) + \chi(f \cdot f_2(x)) + \chi(f_1 \cdot f_2(x))), \text{ and}$$

$$\widehat{S}(f, f_1, f_2) = \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} (\chi(f \cdot f_1(x)) + \chi(f \cdot f_2(x)) + \chi(f_1 \cdot f_2(x))),$$

where for the point at infinity we define

$$\chi(F(\infty)) = \begin{cases} 0 & \deg(F) \text{ odd} \\ 1 & \deg(F) \text{ even, leading coefficient is a square in } \mathbb{F}_q \\ -1 & \deg(F) \text{ even, leading coefficient is not a square in } \mathbb{F}_q \end{cases}.$$

Then, for a curve  $C \in \mathcal{B}_{(g_1,g_2,g_3)}(\mathbb{F}_q)$  defined by a 3-tupla  $(f, f_1, f_2)$  we have that

$$\#C(\mathbb{F}_q) = q + 1 + \widehat{S}(f, f_1, f_2).$$

Hence, we have the equality

$$\frac{|\{C \in \mathcal{B}_{(g_1,g_2,g_3)}(\mathbb{F}_q) : \text{Tr}(\text{Frob}_C) = -M\}|}{|\mathcal{B}_{(g_1,g_2,g_3)}(\mathbb{F}_q)|} = \frac{|\{(f, f_1, f_2) \in \widehat{\mathcal{F}}_{[n,n_1,n_2]} : \widehat{S}(f, f_1, f_2) = M\}|}{|\widehat{\mathcal{F}}_{[n,n_1,n_2]}|}.$$

The goal of this section is to prove the following theorem.

**Theorem 4.1.** *If the three degrees  $n, n_1, n_2$  go to infinity, then we have*

$$\frac{|\{(f, f_1, f_2) \in \widehat{\mathcal{F}}_{[n, n_1, n_2]} : \widehat{S}(f, f_1, f_2) = M\}|}{|\widehat{\mathcal{F}}_{[n, n_1, n_2]}|} = \text{Prob}\left(\sum_{j=1}^{q+1} X_j = M\right),$$

where the  $X_j$  are i.i.d. random variables such that

$$X_i = \begin{cases} -1 & \text{with probability } \frac{3(q+2)}{4(q+3)} \\ 1 & \text{with probability } \frac{6}{4(q+3)} \\ 3 & \text{with probability } \frac{q}{4(q+3)} \end{cases}.$$

More precisely,

$$\frac{|\{(f, f_1, f_2) \in \widehat{\mathcal{F}}_{[n, n_1, n_2]} : \widehat{S}(f, f_1, f_2) = M\}|}{|\widehat{\mathcal{F}}_{[n, n_1, n_2]}|} = \text{Prob}\left(\sum_{j=1}^{q+1} X_j = M\right) \left(1 + O(q^{-\frac{(1-\epsilon)}{2} \min(n, n_1, n_2) + q})\right).$$

The proof of this Theorem runs similarly to the proof of the equivalent statement for hyperelliptic curves (resp.  $l$ -cyclic covers) in [KR09] (resp. [BDFL09]).

**Lemma 4.2.** ([BDFL09, Lemma 4.2]) *For  $0 \leq l \leq q$ , let  $x_1, \dots, x_l$  be distinct elements of  $\mathbb{F}_q$ . Let  $U \in \mathbb{F}_q[t]$  be such that  $U(x_i) \neq 0$  for  $i = 0, \dots, l$ . Let  $a_1, \dots, a_l$  be elements of  $\mathbb{F}_q^*$ . Then the cardinality of the set*

$$\mathcal{S}_d^U(a_1, \dots, a_l) := \{F \in \mathcal{F}_d : (F, U) = 1, F(x_i) = a_i, 1 \leq i \leq l\}$$

is the number

$$\mathcal{S}_d^U(l) = \frac{q^d}{\zeta_q(2)} \left(\frac{q}{q^2 - 1}\right)^l \prod_{P|U} (1 + |P|^{-1})^{-1} \left(1 + O(q^{l-d/2})\right).$$

**Lemma 4.3.** *For  $0 \leq l \leq q$  let  $x_1, \dots, x_l$  be distinct elements of  $\mathbb{F}_q$ . Let  $U \in \mathbb{F}_q[t]$  be such that  $U(x_i) \neq 0$  for  $i = 0, \dots, l$ . Let  $a_1, \dots, a_l, b_1, \dots, b_l$  be elements of  $\mathbb{F}_q^*$ . Then the cardinality of the set*

$$\mathcal{R}_{n_1, n_2}^U(a_1, \dots, a_l, b_1, \dots, b_l) := \{(f_1, f_2) \in \mathcal{F}_{n_1} \times \mathcal{F}_{n_2} : (f_i, U) = (f_1, f_2) = 1, f_1(x_i) = a_i, f_2(x_i) = b_i, 1 \leq i \leq l\}$$

is the number

$$R_{n_1, n_2}^U(l) = \frac{q^{n_1+n_2} L}{\zeta_q^2(2)} \left(\frac{q}{(q-1)^2(q+2)}\right)^l \prod_{P|U} \left(\frac{1}{1+2|P|^{-1}}\right) \left(1 + O(q^{l-\frac{\min(n_1, n_2)}{2}})\right),$$

where  $L := \prod_{P \text{ prime}} (1 - \frac{|P|^{-2}}{(1+|P|^{-1})^2})$ .

*Proof.* By inclusion-exclusion principle (same notations as in [GGL95, Theorem 13.5]), with

$$f(D) = |\{(f_1, f_2) \in \mathcal{F}_{n_1} \times \mathcal{F}_{n_2} : (f_i, U) = 1, D|(f_1, f_2), f_1(x_i) = a_i, f_2(x_i) = b_i, 1 \leq i \leq l\}|,$$

$$g(D) = |\{(f_1, f_2) \in \mathcal{F}_{n_1} \times \mathcal{F}_{n_2} : (f_i, U) = 1, (f_1, f_2) = D, f_1(x_i) = a_i, f_2(x_i) = b_i, 1 \leq i \leq l\}|,$$

where  $D$  is a polynomial in  $\mathbb{F}_q[x]$ , we have

$$R_{n_1, n_2}^U(l) = g(1) = \sum_{D, D(x_i) \neq 0, (D, U) = 1} \mu(D) f(D).$$

But notice that when  $(D, U) = 1$

$$f(D) = |\{(f_1, f_2) \in \mathcal{F}_{n_1 - \deg(D)} \times \mathcal{F}_{n_2 - \deg(D)} : (f_i, UD) = 1, f_1(x_i) = a_i, f_2(x_i) = b_i, 1 \leq i \leq l\}|,$$

hence Lemma 4.2 implies

$$\begin{aligned} f(D) &= S_{n_1 - \deg(D)}^{UD}(l) \cdot S_{n_2 - \deg(D)}^{UD}(l) = \\ &= \frac{q^{n_1 + n_2 - 2\deg(D)}}{\zeta_q^2(2)} \left( \frac{q}{q^2 - 1} \right)^{2l} \prod_{P|UD} (1 + |P|^{-1})^{-2} \left( 1 + O(q^{l + \frac{\deg(D)}{2} - \frac{\min(n_1, n_2)}{2}}) \right). \end{aligned}$$

So, one has

$$\begin{aligned} R_{n_1, n_2}^U(l) &= \sum_{D, D(x_i) \neq 0, (D, U)=1} \mu(D) f(D) = \\ &= \frac{q^{n_1 + n_2}}{\zeta_q^2(2)} \left( \frac{q}{q^2 - 1} \right)^{2l} \prod_{P|U} (1 + |P|^{-1})^{-2} \sum_{\substack{D(x_i) \neq 0, (D, U)=1 \\ \deg(D) \leq \min(n_1, n_2)}} \mu(D) |D|^{-2} \prod_{P|D} (1 + |P|^{-1})^{-2} \left( 1 + O(q^{l - \frac{\min(n_1, n_2)}{2}}) \right). \end{aligned}$$

Now, we observe that

$$\begin{aligned} \sum_{\substack{D(x_i) \neq 0, (D, U)=1 \\ \deg(D) \leq \min(n_1, n_2)}} \mu(D) |D|^{-2} \prod_{P|D} (1 + |P|^{-1})^{-2} &= \\ &= \sum_{D, D(x_i) \neq 0, (D, U)=1} \mu(D) |D|^{-2} \prod_{P|D} (1 + |P|^{-1})^{-2} + O(q^{-2\min(n_1, n_2)}), \end{aligned}$$

where we have that

$$\begin{aligned} \sum_{D, D(x_i) \neq 0, (D, U)=1} \mu(D) |D|^{-2} \prod_{P|D} (1 + |P|^{-1})^{-2} &= \\ &= \left( \frac{(q+1)^2}{q(q+2)} \right)^l \prod_{P|U} \left( \frac{1 + 2|P|^{-1}}{(1 + |P|^{-1})^2} \right)^{-1} \prod_{P \text{ prime}} \left( 1 - \frac{|P|^{-2}}{(1 + |P|^{-1})^2} \right) = \left( \frac{(q+1)^2}{q(q+2)} \right)^l \prod_{P|U} \left( \frac{1 + 2|P|^{-1}}{(1 + |P|^{-1})^2} \right)^{-1} L. \end{aligned}$$

We can prove that  $0 < L < 1$  (see next Remark 4.4). So, finally

$$R_{n_1, n_2}^U(l) = \frac{q^{n_1 + n_2} L}{\zeta_q^2(2)} \left( \frac{q}{(q-1)^2(q+2)} \right)^l \prod_{P|U} \left( \frac{1}{1 + 2|P|^{-1}} \right) \left( 1 + O(q^{l - \frac{\min(n_1, n_2)}{2}}) \right).$$

□

**Remark 4.4.** We need to prove that the infinite product  $\prod_{P \text{ prime}} (1 - \frac{|P|^{-2}}{(1 + |P|^{-1})^2})$  converges to a real number  $L$  such that  $0 < L < 1$ . The Prime Polynomial Theorem implies that this is equivalent to prove that the infinite product

$$\prod_{\nu \geq 1} \left( 1 - \frac{1}{(q^\nu + 1)^2} \right)^{\frac{q^\nu}{\nu}}$$

converges to a positive real number  $\tilde{L}$ , in particular, we will see that  $0 < \tilde{L} < 1$  (remember that  $q \geq 3$ ).

Because  $\left( 1 - \frac{1}{(q^\nu + 1)^2} \right)^{\frac{q^\nu}{\nu}} < 1$ , we have that  $\tilde{L} < 1$ . In order to prove that  $0 < \tilde{L}$ , and since for  $z \in (0, 1)$  we have  $\log(1 - z) \geq \frac{z}{z-1}$ , it is enough to prove that

$$\sum_{\nu \geq 1} \frac{q^\nu}{\nu} \frac{\frac{1}{(q^\nu + 1)^2}}{\frac{1}{(q^\nu + 1)^2} - 1} = - \sum_{\nu \geq 1} \frac{1}{\nu} \cdot \frac{1}{q^\nu + 2}$$



is convergent. Indeed, we have

$$0 \leq \sum_{\nu \geq 1} \frac{1}{\nu} \cdot \frac{1}{q^\nu + 2} \leq \sum_{\nu \geq 1} \frac{1}{\nu 3^\nu} = \log \frac{3}{2}.$$

Thus,

$$\prod_{\nu \geq 1} \left( 1 - \frac{1}{(q^\nu + 1)^2} \right)^{\frac{q^\nu}{\nu}} \geq \frac{2}{3}.$$

**Proposition 4.5.** *For  $0 \leq l \leq q$ , let  $x_1, \dots, x_l$  be distinct elements of  $\mathbb{F}_q$ , and  $a_1, \dots, a_l, b_1, \dots, b_l$  be elements of  $\mathbb{F}_q^*$ . Then, for any  $1 > \epsilon > 0$ , we have*

$$\begin{aligned} & |\{(f, f_1, f_2) \in \mathcal{F}_{(n, n_1, n_2)} : f(x_i)f_1(x_i) = a_i, f(x_i)f_2(x_i) = b_i, 1 \leq i \leq l\}| = \\ & = \frac{KLq^{n_1+n_2+n}}{\zeta_q^3(2)} \left( \frac{q}{(q-1)^2(q+3)} \right)^l (1 + O(q^{-(1-\epsilon)n+el} + q^{-n-\frac{\min(n_1, n_2)}{2}+l})), \end{aligned}$$

where  $K := \prod_P \left( \frac{1+3|P|^{-1}}{(1+|P|^{-1})(1+2|P|^{-1})} \right)$ .

*Proof.* First we observe that

$$\begin{aligned} & |\{(f, f_1, f_2) \in \mathcal{F}_{(n, n_1, n_2)} : f(x_i)f_1(x_i) = a_i, f(x_i)f_2(x_i) = b_i, 1 \leq i \leq l\}| = \\ & = \sum_{\substack{f \in \mathcal{F}_n \\ f(x_i) \neq 0}} \sum_{\substack{f_1 \in \mathcal{F}_{n_1} \\ f_1(x_i) = a_i f(x_i)^{-1} \\ (f, f_1) = 1}} \sum_{\substack{f_2 \in \mathcal{F}_{n_1} \\ f_2(x_i) = b_i f(x_i)^{-1} \\ (f f_1, f_2) = 1}} 1 = \\ & = \sum_{f \in \mathcal{F}_n, f(x_i) \neq 0} R_{n_1, n_2}^f(l). \end{aligned}$$

Using Lemma 4.3 we have that

$$\begin{aligned} & |\{(f, f_1, f_2) \in \mathcal{F}_{(n, n_1, n_2)} : f(x_i)f_1(x_i) = a_i, f(x_i)f_2(x_i) = b_i, 1 \leq i \leq l\}| = \\ & = \frac{q^{n_1+n_2}L}{\zeta_q^2(2)} \left( \frac{q}{(q-1)^2(q+2)} \right)^l \sum_{U \in \mathcal{F}_n, U(x_i) \neq 0} \prod_{P|U} \frac{1}{1+2|P|^{-1}} + O(q^{n_1+n_2-\frac{\min(n_1, n_2)}{2}-l}) = \\ & = \frac{q^{n_1+n_2}L}{\zeta_q^2(2)} \left( \frac{q}{(q-1)^2(q+2)} \right)^l \sum_{\deg(U)=n} c(U) + O(q^{n_1+n_2-\frac{\min(n_1, n_2)}{2}-l}), \end{aligned}$$

where for any polynomial  $U$ , we define

$$c(U) = \begin{cases} \mu^2(U) \prod_{P|U} \frac{1}{1+2|P|^{-1}} & U(x_i) \neq 0 \\ 0 & \text{otherwise} \end{cases}.$$

In order to evaluate  $\sum_{\deg(U)=n} c(U)$ , we consider the Dirichlet series

$$\begin{aligned} G(w) &= \sum_U \frac{c(U)}{|U|^w} = \prod_{P, P(x_i) \neq 0} \left( 1 + \frac{1}{|P|^w} \cdot \frac{|P|}{(|P|+2)} \right) = \\ &= \frac{\zeta_q(w)}{\zeta_q(2w)} H(w) \left( 1 + \frac{1}{q^{w-1}(q+2)} \right)^{-l}, \end{aligned}$$

with

$$H(w) = \prod_P \left( 1 - \frac{2}{(1+|P|^w)(|P|+2)} \right).$$

Notice that  $H(w)$  converges absolutely for  $\operatorname{Re}(w) > 0$ , and  $G(w)$  is meromorphic for  $\operatorname{Re}(w) > 0$  with simple poles at the points  $w$  where  $\zeta_q(w) = (1 - q^{1-w})^{-1}$  has poles, that is,  $1 + i\frac{2\pi n}{\log q}$ . Thus,  $G(w)$  has a simple pole at  $w = 1$  with residue

$$\frac{K}{\zeta_q(2)\log(q)} \left(\frac{q+2}{q+3}\right)^l,$$

where  $K = H(1)$ .

Using Theorem 17.1 of [Ros02], which is the function field version of the Wiener-Ikehara Tauberian Theorem, we get that

$$\sum_{\deg(U)=n} c(U) = \frac{K}{\zeta_q(2)} \left(\frac{q+2}{q+3}\right)^l q^n + O_q(q^{\epsilon n}),$$

for all  $\epsilon \geq 0$  and where, looking at the proof of the theorem and proceeding as in Proposition 4.3 in [BDFL09], we can exchange  $O_q(q^{\epsilon n})$  by  $O(q^{\epsilon(n+l)})$ .  $\square$

**Corollary 4.6.** *For  $0 \leq l \leq q$ , let  $x_1, \dots, x_l$  be distinct elements of  $\mathbb{F}_q$ , and let  $a_1, \dots, a_l, b_1, \dots, b_l$  be elements of  $\mathbb{F}_q$  such that  $a_1 = \dots = a_{r_0} = b_1 = \dots = b_{r_0} = 0$ ,  $a_{r_0+1} = \dots = a_{r_0+r_1} = 0 = b_{r_0+r_1+1} = \dots = b_{r_0+r_1+r_2}$  and  $b_{r_0+1}, \dots, b_{r_0+r_1}, a_{r_0+r_1+1}, \dots, a_{r_0+r_1+r_2}, a_j, b_j \neq 0$  if  $j > r_0 + r_1 + r_2 = m$ . Then, for every  $\epsilon > 0$ , the number*

$$\frac{|\{(f, f_1, f_2) \in \mathcal{F}_{(n, n_1, n_2)} : f(x_i)f_1(x_i) = a_i, f(x_i)f_2(x_i) = b_i, f_1(x_i)f_2(x_i) = c_i, 1 \leq i \leq l\}|}{|\mathcal{F}_{(n, n_1, n_2)}|},$$

where  $f(x_i)^2 c_i = a_i b_i$ , is equal to

$$\left(\frac{1}{(q-1)(q+3)}\right)^m \left(\frac{q}{(q-1)^2(q+3)}\right)^{l-m} \left(1 + O(q^{-\frac{(1-\epsilon)}{2} \min(n, n_1, n_2) + l})\right).$$

*Proof.* Let us write  $f = (x - x_1) \dots (x - x_{r_0}) f'$ ,  $f_1 = (x - x_{r_0+1}) \dots (x - x_{r_0+r_1}) f'_1$ , and  $f_2 = (x - x_{r_0+r_1+1}) \dots (x - x_{r_0+r_1+r_2}) f'_2$ . Now, apply Proposition 4.5 to the 3-tuple  $(f', f'_1, f'_2)$  and sum.  $\square$

**Corollary 4.7.** *With notations as in Corollary 4.6, the number*

$$\frac{|\{(f, f_1, f_2) \in \mathcal{F}_{(n, n_1, n_2)} : \chi(f(x_i)f_1(x_i)) = e_i^1, \chi(f(x_i)f_2(x_i)) = e_i^2, \chi(f_1(x_i)f_2(x_i)) = e_i, 1 \leq i \leq l\}|}{|\mathcal{F}_{(n, n_1, n_2)}|},$$

where  $e_i^1, e_i^2, e_i \in \{-1, 0, 1\}$ ,  $\chi(f(x_i)^2)e_i = e_i^1 e_i^2$ , and exactly  $2m$  of them are equal to zero, is equal to

$$\begin{aligned} C_m^l &= \left(\frac{q-1}{2}\right)^m \left(\frac{q-1}{2}\right)^{2(l-m)} \left(\frac{1}{(q-1)(q+3)}\right)^m \left(\frac{q}{(q-1)^2(q+3)}\right)^{l-m} \left(1 + O(q^{-\frac{(1-\epsilon)}{2} \min(n, n_1, n_2) + l})\right) \\ &= \left(\frac{1}{2(q+3)}\right)^m \left(\frac{q}{4(q+3)}\right)^{l-m} \left(1 + O(q^{-\frac{(1-\epsilon)}{2} \min(n, n_1, n_2) + l})\right). \end{aligned}$$

**Corollary 4.8.** *For  $0 \leq l \leq q$ , let  $x_1, \dots, x_l$  be distinct elements of  $\mathbb{P}^1(\mathbb{F}_q)$ , and let  $e_i^1, e_i^2, e_i \in \{-1, 0, 1\}$  be such that  $\chi(f(x_i)^2)e_i = e_i^1 e_i^2$ , where exactly  $2m$  of them are equal to zero. Then*

$$\frac{|\{(f, f_1, f_2) \in \widehat{\mathcal{F}}_{[n, n_1, n_2]} : \chi(f(x_i)f_1(x_i)) = e_i^1, \chi(f(x_i)f_2(x_i)) = e_i^2, \chi(f_1(x_i)f_2(x_i)) = e_i\}|}{|\widehat{\mathcal{F}}_{[n, n_1, n_2]}|}$$

is also equal to the number  $C_m^l$  defined in Corollary 4.7.

*Proof.* Distinguish the case in which some  $x_j$  is the point at infinity or not. Generalize Corollary 4.7 for the sets  $\widehat{\mathcal{F}}_{(n,n_1,n_2)}$  looking at the symmetry observed in Remark 2.7, and add for the different components of  $\widehat{\mathcal{F}}_{[n,n_1,n_2]}$ .  $\square$

*Proof.* (of Theorem 4.1) Apply Corollary 4.8 in order to compute

$$\begin{aligned}
& \frac{|\{(f, f_1, f_2) \in \widehat{\mathcal{F}}_{[n,n_1,n_2]} : \widehat{S}(f, f_1, f_2) = M\}|}{|\widehat{\mathcal{F}}_{[n,n_1,n_2]}|} = \\
&= \sum_{\epsilon_1, \dots, \epsilon_{q+1} \in \{-1, 1, 3\}, \sum \epsilon_i = M} \sum_{j=0}^{N-1} \binom{N-1}{j} 3^{N_1+N-1} C_{N_1+j}^{q+1} = \\
&= \sum_{\epsilon_1, \dots, \epsilon_{q+1} \in \{-1, 1, 3\}, \sum \epsilon_i = M} \left( \frac{6}{4} \frac{1}{q+3} \right)^{N_1} \left( \frac{3}{4} \frac{q+2}{q+3} \right)^{N-1} \left( \frac{1}{4} \frac{q}{q+3} \right)^{N_3} \left( 1 + O(q^{-\frac{(1-\epsilon)}{2} \min(n, n_1, n_2) + q}) \right) \\
&= \text{Prob} \left( \sum_1^{q+1} X_i = M \right) \left( 1 + O(q^{-\frac{(1-\epsilon)}{2} \min(n, n_1, n_2) + q}) \right),
\end{aligned}$$

where we use the notation  $N_i$  for the number of elements equal to  $i$  in the set  $\{\epsilon_1, \dots, \epsilon_{q+1}\}$ .  $\square$

## 5. AVERAGES AND MOMENTS SEQUENCES

We want to compute the moments of  $\text{Tr}(\text{Frob}_C)/\sqrt{1+q}$ . That is, the  $k$ th moments

$$M_k(q, g_1, g_2, g_3) = \frac{1}{|\mathcal{B}_{(g_1, g_2, g_3)}(\mathbb{F}_q)|} \sum_{C \in \mathcal{B}_{(g_1, g_2, g_3)}(\mathbb{F}_q)} \left( \frac{\text{Tr}(\text{Frob}_C)}{\sqrt{1+q}} \right)^k.$$

**Theorem 5.1.** *With notation in Theorem 4.1, we have*

$$M_k(q, g_1, g_2, g_3) = \mathbb{E} \left( \left( \frac{1}{\sqrt{1+q}} \sum_{i=1}^{1+q} X_i \right)^k \right) + O(q^{-\frac{1-\epsilon}{2} \min(n, n_1, n_2) + k}).$$

**Corollary 5.2.** *If  $g_1, g_2, g_3$  and  $q$  tend to infinity, then the moments of  $\text{Tr}(\text{Frob}_C)/\sqrt{1+q}$ , as  $C$  runs over the irreducible component  $\mathcal{B}_{(g_1, g_2, g_3)}(\mathbb{F}_q)$  of the moduli space  $\mathcal{B}_g(\mathbb{F}_q)$ , are asymptotically Gaussian with mean 0 and variance 1.*

*Proof.* Since the moments of a sum of bounded i.i.d. random variables converge to the Gaussian moments ([Bil95, Sec. 30]), it follows that, as all  $q, g_1, g_2, g_3$  go to  $\infty$ ,  $M_k(q, g_1, g_2, g_3)$  agrees with Gaussian moments for all  $k$ . Then, Theorem 30.2 in [Bil95] implies the corollary.  $\square$

*Proof.* (of Theorem 5.1) We can write the  $k$ th moment as

$$\begin{aligned}
M_k(q, g_1, g_2, g_3) &= (-1)^k \frac{q(q^2-1)}{|\widehat{\mathcal{F}}_{[2g_1+2, 2g_2+2, 2g_3+2]}|} \sum_{(f_1, f_2, f_3) \in \widehat{\mathcal{F}}_{[2g_1+2, 2g_2+2, 2g_3+2]}} (\widehat{S}(f_1, f_2, f_3))^k = \\
&= \frac{(-1)^k q(q^2-1)}{|\widehat{\mathcal{F}}_{[2g_1+2, 2g_2+2, 2g_3+2]}|} \sum_{(f_1, f_2, f_3) \in \widehat{\mathcal{F}}_{[2g_1+2, 2g_2+2, 2g_3+2]}} \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} (\chi(f \cdot f_1(x)) + \chi(f \cdot f_2(x)) + \chi(f_1 \cdot f_2(x)))^k = \\
&= (-1)^k q(q^2-1) \sum_{l=1}^k c(k, l) \sum_{(x, b) \in P_{k, l}} \frac{1}{|\widehat{\mathcal{F}}_{[2g_1+2, 2g_2+2, 2g_3+2]}|} \sum_{(f_1, f_2, f_3) \in \widehat{\mathcal{F}}_{[2g_1+2, 2g_2+2, 2g_3+2]}} B(x, b, f_1, f_2, f_3),
\end{aligned}$$

where, borrowing the notation in [BDFL09, Sec. 5]

$$P_{k,l} = \left\{ (x, b) : x = (x_1, \dots, x_l) \in \mathbb{P}^1(\mathbb{F}_q)^l, x'_i \text{'s distinct}, b = (b_1, \dots, b_l) \in \mathbb{Z}_{>0}^l, \sum_{i=1}^l b_i = k \right\},$$

$$B(x, b, f_1, f_2, f_3) = \prod_{i=1}^l (\chi(f \cdot f_1(x_i)) + \chi(f \cdot f_2(x_i)) + \chi(f_1 \cdot f_2(x_i)))^{b_i}$$

and  $c(k, l)$  is a certain combinatorial factor. We do not need exact formulas for it, but as it was notice in [BDFL09]

$$\sum_{l=1}^k c(k, l) \sum_{(x, b) \in P_{k, l}} 1 = (q+1)^k. \quad (5.1)$$

Fix a vector  $(x, b) \in P_{(k, l)}$ . Then, the number

$$\begin{aligned} \sum_{(f_1, f_2, f_3) \in \widehat{\mathcal{F}}_{[2g_1+2, 2g_2+2, 2g_3+2]}} \frac{B(x, b, f_1, f_2, f_3)}{|\widehat{\mathcal{F}}_{[2g_1+2, 2g_2+2, 2g_3+2]}|} &= \sum_{\substack{(\epsilon_1, \dots, \epsilon_l) \\ \epsilon_i \in \{-1, 1, 3\}}} (\prod P_{\epsilon_i}) (\prod \epsilon_i^{b_i}) = \\ \sum_{\substack{(\epsilon_1, \dots, \epsilon_l) \\ \epsilon_i \in \{-1, 1, 3\}}} (\prod P_{\epsilon_i} \epsilon_i^{b_i}) &= \prod_i \left( \frac{3^{b_i} q + 6 + (-1)^{b_i} 3(q+2)}{4(q+3)} \right) (1 + O(q^{-\frac{1-\epsilon}{2} \min(n, n_1, n_2) + l})) \end{aligned}$$

We obtain that

$$M_k(q, g_1, g_2, g_3) = (-1)^k q(q^2-1) \sum_{l=1}^k c(k, l) \sum_{(x, b) \in P_{k, l}} \prod_i \left( \frac{3^{b_i} q + 6 + (-1)^{b_i} 3(q+2)}{4(q+3)} \right) (1 + O(q^{-\frac{1-\epsilon}{2} \min(n, n_1, n_2) + k})).$$

where the error term is estimated using 5.1.

On the other hand, the corresponding moment of the normalized sum of our random variables is

$$\mathbb{E} \left( \left( \frac{1}{\sqrt{1+q}} \sum_{i=1}^{1+q} X_i \right)^k \right) = \frac{1}{(1+q)^{k/2}} \sum_{l=1}^k \sum_{(i, b) \in A_{k, l}} \mathbb{E}(X_{i_1}^{b_1} \dots X_{i_l}^{b_l}),$$

where

$$A_{k, l} = \left\{ (i, b) : i = (i_1, \dots, i_l), 1 \leq i_j \leq q+1, i'_j \text{'s distinct}, b = (b_1, \dots, b_l) \in \mathbb{Z}_{>0}^l, \sum_{i=1}^l b_i = k \right\}$$

is clearly isomorphic to  $P_{k, l}$ .

Since

$$\mathbb{E}(X_i^b) = \frac{3^b q + 6 + (-1)^b 3(q+2)}{4(q+3)}$$

and  $X_1, \dots, X_{1+q}$  are independent, we get the equality in the statement of the theorem.  $\square$

## 6. GENERAL CASE: THE FAMILY OF $r$ -QUADRATIC CURVES

**Definition 6.1.** Let  $r \geq 1$  be an integer. We call  $r$ -quadratic curve a non-singular projective curve  $C/\mathbb{F}_q$  together with a morphism  $\varphi : C \rightarrow \mathbb{P}_{\mathbb{F}_q}^1$  defined over  $\mathbb{F}_q$  such that it induces a function field extension with Galois group

$$\text{Gal}(\mathbb{F}_q(C)/\mathbb{F}_q(t)) \simeq (\mathbb{Z}/2\mathbb{Z})^r$$

Note that when  $r = 1$  and  $r = 2$  we find respectively the definition of hyperelliptic curve and that of biquadratic curve given in Section 2.

The family of  $r$ -quadratic curves is studied in [GP05a] where it is proved that when we consider the family of this curve defined over  $\mathbb{F}_q$  we obtain a coarse moduli space over  $\mathbb{Z}[1/2]$ . In the same paper a formula for the genus of an  $r$ -quadratic curve is also proved.

**Proposition 6.2.** *Let  $r \geq 1$  be an integer and let  $C/\mathbb{F}_q$  be an  $r$ -quadratic curve.*

(1) *An affine model of  $C$  in  $\mathbb{A}^{r+1}$  is given by*

$$C : \begin{cases} y_1^2 = h_1(t) \\ \dots \\ y_r^2 = h_r(t) \end{cases}$$

*where each  $h_i$  is square-free and different (up to squares) from  $\prod_{j \in J} h_j$ , for every non-empty subset  $J \subseteq \{1, \dots, r\}$ ,  $J \neq \{i\}$ .*

(2) *For every non-empty  $J \subseteq \{1, \dots, r\}$ , the affine equation*

$$y^2 = \prod_{j \in J} h_j(t)$$

*defines a quadratic subextension of  $\mathbb{F}_q(C)/k$  and every quadratic subextension of  $\mathbb{F}_q(C)/k$  is obtained in this way, so there are  $2^r - 1$  of them.*

(3) *If we write  $C_J$  for the hyperelliptic curve given by the affine equation  $y^2 = \prod_{j \in J} h_j(t)$ , then*

$$g(C) = \sum_{J \subseteq \{1, \dots, r\}} g(C_J).$$

Next Theorem gives a convenient way of describing the family of  $r$ -quadratic curves, and it is the key point to compute the distribution of the Frobenius traces.

**Theorem 6.3.** *There exists a one-to-one correspondence between the set of  $r$ -quadratic extensions of  $k$  and the set of unordered  $2^r - 1$ -tuples of square-free and pairwise coprime polynomials.*

*Proof.* Let  $K = k(\sqrt{h_1}, \dots, \sqrt{h_r})$  be an  $r$ -quadratic extension. We associate to such an extension, a  $2^r - 1$ -tuple  $(f_1, \dots, f_{2^r-1})$  of square-free and pairwise coprime polynomials in the following way: for every  $i \in \{1, \dots, 2^r - 1\}$ , we write  $B_1^i \dots B_r^i$  for the representation of the integer  $i$  in base 2 (so  $B_j^i \in \{1, 0\}$  for every  $1 \leq j \leq r$ ) and we define  $m_i$  to be the greatest common divisor of all polynomials  $h_j$  such that the  $B_j = 1$ .

We then define the polynomials  $f_i$  as the maximum factor in the decomposition of  $m_i$  which is coprime to all the  $h_j$  such that  $B_j^i = 0$ . Notice that, in particular,  $f_{2^r-1} = (h_1, \dots, h_r)$ .

Viceversa, given a tuple  $(f_1, \dots, f_{2^r-1})$  of square-free and pairwise coprime polynomials, we define the  $r$ -quadratic extension  $k(\sqrt{h_1}, \dots, \sqrt{h_r})$ , where  $h_i$  is defined to be the product of the  $f_j$  such that the  $i$ -th digit of  $j$  in base 2 is 1, i.e.  $B_i^j = 1$ .  $\square$

Notice that, with notations of Theorem 6.3, we have that  $f_{2^r-1} = (h_1, \dots, h_r)$ .

After Theorem 6.3, we are led to define the following sets:

$$\mathcal{F}_{(n_1, \dots, n_{2^r-1})} := \{(f_1, \dots, f_{2^r-1}) \in \mathcal{F}_{n_1} \times \dots \times \mathcal{F}_{n_{2^r-1}} : (f_i, f_j) = 1, \ i, j = 1, \dots, 2^r - 1, i \neq j\},$$

$$\widehat{\mathcal{F}}_{(n_1, \dots, n_{2^r-1})} := \{(f_1, \dots, f_{2^r-1}) \in \widehat{\mathcal{F}}_{n_1} \times \dots \times \widehat{\mathcal{F}}_{n_{2^r-2}} \times \mathcal{F}_{n_{2^r-1}} : (f_i, f_j) = 1, \ i, j = 1, \dots, 2^r - 1, i \neq j\},$$

It is easy to prove that if  $C$  is an  $r$ -quadratic curve whose affine model is given by equations  $y_i^2 = h_i(t)$ ,  $i = 1, \dots, r$ , then

$$\#C(\mathbb{F}_q) = \sum_{x \in \mathbb{P}_{\mathbb{F}_q}^1} \prod_{i=1}^r (1 + \chi(h_i(x))).$$

Now, we express this formula in terms of the polynomials  $f_1, \dots, f_{2^r-1}$  defined in the proof of Theorem 6.3.

Let us fix  $(f_1, \dots, f_{2^r-1}) \in \widehat{\mathcal{F}}_{(n_1, \dots, n_{2^r-1})}$ . For every  $i \in \{1, \dots, 2^r - 1\}$ , we define the polynomial  $p_i$  as the square-free part of the product of the polynomials  $f_j$  such that the relation between the representations in base 2 of  $i$  and  $j$  is the following:  $B_k^i = 1 \Rightarrow B_k^j = 1$ . It is immediate to see that, inside the correspondence of Theorem 6.3, the square-free polynomials  $p_1, \dots, p_{2^r-1}$  define all the quadratic subextensions of the  $r$ -quadratic extension defined by the tuple  $(f_1, \dots, f_{2^r-1})$ .

Then we define

$$\widehat{S}(f_1, \dots, f_{2^r-1}) := \sum_{x \in \mathbb{P}^1} \sum_{i=1}^{2^r-1} \chi(p_i(x))$$

and we can rewrite

$$\#C(\mathbb{F}_q) = \sum_{x \in \mathbb{P}^1} \prod_{i=1}^{2^r-1} (1 + \chi(p_i(x))) = q + 1 + \widehat{S}(f_1, \dots, f_{2^r-1}).$$

When  $r = 2$  we find the formula of Section 4.

**Lemma 6.4.** *Let  $n_1, \dots, n_\beta$  be positive integers. For  $0 \leq l \leq q$ , let  $x_1, \dots, x_l$  be distinct elements of  $\mathbb{F}_q$ . Let  $U \in \mathbb{F}_q[X]$  be such that  $U(x_i) \neq 0$  for  $i = 0, \dots, l$ . Let be  $a_1^1, \dots, a_l^1, \dots, a_1^\beta, \dots, a_l^\beta \in \mathbb{F}_q^*$ . The number of elements in the set*

$$\mathcal{R}_{n_1, \dots, n_\beta}^U((a_1^j, \dots, a_l^j)_{1 \leq j \leq \beta}) := \{(f_1, \dots, f_\beta) \in \mathcal{F}_{n_1} \times \dots \times \mathcal{F}_{n_\beta} : \\ (f_j, U) = 1, (f_j, f_k)_{k \neq j} = 1, f_j(x_i) = a_i^j, 1 \leq i \leq l, 1 \leq j, k \leq \beta\}$$

is the number

$$R_{n_1, \dots, n_\beta}^U(l) = \frac{q^{n_1 + \dots + n_\beta} L_\beta}{\zeta_q^\beta(2)} \left( \frac{q}{(q-1)^\beta (q+\beta)} \right)^l \prod_{P|U} \left( \frac{1}{1 + \beta|P|^{-1}} \right) (1 + O(q^{l - \frac{\min(n_1, \dots, n_\beta)}{2}})),$$

where the constant

$$L_\beta := \prod_{P \text{ prime}} \left( \frac{|P|^{\beta-1}(|P| + \beta)}{(|P| + 1)^\beta} \right).$$

In a similar way to Remark 4.4, we can see that  $L_\beta$  is bounded.

*Proof.* We will prove it by induction on  $\beta$ . We find Lemma 4.2 for  $\beta = 1$ , and for  $\beta = 2$  we find Lemma 4.3. Assume that the equality of the statement is true for  $\beta - 1$ .

By inclusion-exclusion principle, with

$$f(D) = |\{(f_1, \dots, f_\beta) \in \mathcal{R}_{n_1, \dots, n_{\beta-1}}^U((a_1^j, \dots, a_l^j)_{1 \leq j \leq \beta-1}) \times \mathcal{S}_{n_\beta}^U(a_1^\beta, \dots, a_l^\beta) : D|(f_1 \dots f_{\beta-1}, f_\beta)\}|,$$

$$g(D) = |\{(f_1, \dots, f_\beta) \in \mathcal{R}_{n_1, \dots, n_{\beta-1}}^U((a_1^j, \dots, a_l^j)_{1 \leq j \leq \beta-1}) \times \mathcal{S}_{n_\beta}^U(a_1^\beta, \dots, a_l^\beta) : D = (f_1 \dots f_{\beta-1}, f_\beta)\}|,$$

we have

$$R_{n_1, \dots, n_\beta}^U(l) = g(1) = \sum_{D, D(x_i) \neq 0, (D, U)=1} \mu(D) f(D).$$

But notice that when  $(D, U) = 1$  and  $D$  is square-free

$$f(D) = \prod_{P|D} (\beta - 1) \cdot R_{n_1, \dots, n_{\beta-1} - \deg(D)}^{UD}(l) \cdot S_{n_\beta - \deg(D)}^{UD}(l)$$

hence, by induction hypothesis,

$$f(D) = \frac{q^{n_1 + \dots + n_\beta} L_{\beta-1}}{\zeta_q^\beta(2)} \left( \frac{q^2}{(q^2 - 1)(q - 1)^{\beta-1}(q + \beta - 1)} \right)^l \\ \prod_{P|U} \frac{1}{(1 + (\beta - 1)|P|^{-1})(1 + |P|^{-1})} \prod_{P|D} \frac{(\beta - 1)|P|^{-2}}{(1 + (\beta - 1)|P|^{-1})(1 + |P|^{-1})} \left( 1 + O(q^{l + \frac{\deg(D)}{2} - \frac{\min(n_1, \dots, n_\beta)}{2}}) \right).$$

So, one has

$$\begin{aligned}
R_{n_1, \dots, n_\beta}^U(l) &= \sum_{D, D(x_i) \neq 0, (D, U)=1} \mu(D) f(D) = \\
&= \frac{q^{n_1 + \dots + n_\beta} L_{\beta-1}}{\zeta_q^\beta(2)} \left( \frac{q^2}{(q^2-1)(q-1)^{\beta-1}(q+\beta-1)} \right)^l \prod_{P|U} \frac{1}{(1+(\beta-1)|P|^{-1})(1+|P|^{-1})} \\
&\quad \sum_{\substack{D(x_i) \neq 0, (D, U)=1 \\ \deg(D) \leq \min(n_1, \dots, n_\beta)}} \mu(D) \prod_{P|D} \frac{(\beta-1)|P|^{-2}}{(1+(\beta-1)|P|^{-1})(1+|P|^{-1})} \left( 1 + O(q^{l - \frac{\min(n_1, \dots, n_\beta)}{2}}) \right).
\end{aligned}$$

Now, we observe that

$$\begin{aligned}
&\sum_{\substack{D(x_i) \neq 0, (D, U)=1 \\ \deg(D) \leq \min(n_1, \dots, n_\beta)}} \mu(D) \prod_{P|D} \frac{(\beta-1)|P|^{-2}}{(1+(\beta-1)|P|^{-1})(1+|P|^{-1})} = \\
&\quad \sum_{D, D(x_i) \neq 0, (D, U)=1} \mu(D) \prod_{P|D} \frac{(\beta-1)|P|^{-2}}{(1+(\beta-1)|P|^{-1})(1+|P|^{-1})} + O(q^{-2\min(n_1, \dots, n_\beta)}),
\end{aligned}$$

where we have that

$$\begin{aligned}
&\sum_{D, D(x_i) \neq 0, (D, U)=1} \mu(D) \prod_{P|D} \frac{(\beta-1)|P|^{-2}}{(1+(\beta-1)|P|^{-1})(1+|P|^{-1})} = \\
&= \left( 1 - \frac{(\beta-1)q^{-2}}{(1+(\beta-1)q^{-1})(1+q^{-1})} \right)^{-l} \prod_{P|U} \left( 1 - \frac{(\beta-1)|P|^{-2}}{(1+(\beta-1)|P|^{-1})(1+|P|^{-1})} \right)^{-1} \prod_{P \text{ prime}} \left( 1 - \frac{(\beta-1)|P|^{-2}}{(1+(\beta-1)|P|^{-1})(1+|P|^{-1})} \right) = \\
&= \left( \frac{(q+\beta-1)(q+1)}{q(q+\beta)} \right)^l \prod_{P|U} \left( \frac{\beta|P|^{-1}+1}{(1+(\beta-1)|P|^{-1})(1+|P|^{-1})} \right)^{-1} \prod_{P \text{ prime}} \frac{\beta|P|^{-1}+1}{(1+(\beta-1)|P|^{-1})(1+|P|^{-1})}.
\end{aligned}$$

So, the result follows.  $\square$

**Proposition 6.5.** For  $0 \leq l \leq q$ , let  $x_1, \dots, x_l$  be distinct elements of  $\mathbb{F}_q$ , and let be  $a_1^1, \dots, a_l^1, \dots, a_1^r, \dots, a_l^r \in \mathbb{F}_q^*$ . Then for any  $1 > \epsilon > 0$ , we have

$$\begin{aligned}
&|\{(f_1, \dots, f_{2^r-1}) \in \mathcal{F}_{(n_1, \dots, n_{2^r-1})} : h_j(x_i) = a_i^j, 1 \leq i \leq l, 1 \leq j \leq r\}| = \\
&= \frac{q^{n_1 + \dots + n_{2^r-1}} L_{2^r-2}}{\zeta_q^{2^r-1}(2)} \left( \frac{q}{(q-1)^r(q+2^r-1)} \right)^l (1 + O(q^{l - \frac{\min(n_1, \dots, n_\beta)}{2}})).
\end{aligned}$$

*Proof.* Apply previous Lemma with  $\beta = 2^r - 1$  and  $U(x) = 1$ . Notice that the value of the polynomials  $h_i$  can be fixed by controlling the value of  $r$  of the  $f_j$  polynomials, so we need to multiply the previous number by  $(q-1)^{l(2^r-1-r)}$ .  $\square$

**Corollary 6.6.** For  $0 \leq l \leq q$ , let  $x_1, \dots, x_l$  be distinct elements of  $\mathbb{F}_q$ , and let  $a_1^1, \dots, a_l^1, \dots, a_1^r, \dots, a_l^r$  be elements in  $\mathbb{F}_q$  such that for exactly  $m$  values of  $i$  we have  $\prod_{i=1}^r a_i^j = 0$ . Then, for any  $1 > \epsilon > 0$ , we have

$$\begin{aligned}
&|\{(f_1, \dots, f_{2^r-1}) \in \mathcal{F}_{(n_1, \dots, n_{2^r-1})} : h_j(x_i) = a_i^j, 1 \leq i \leq l, 1 \leq j \leq r\}| = \\
&= \frac{q^{n_1 + \dots + n_{2^r-1}} L_{2^r-2}}{\zeta_q^{2^r-1}(2)} \left( \frac{q}{(q-1)^r(q+2^r-1)} \right)^{l-m} \left( \frac{1}{(q-1)^{r-1}(q+2^r-1)} \right)^m (1 + O(q^{l - \frac{\min(n_1, \dots, n_\beta)}{2}})).
\end{aligned}$$

*Proof.* According to the values of  $a_i^j$  we can decide which of the polynomials  $f_k$  should satisfy  $f_j(x_i) = 0$ , see Theorem 6.3. Write  $f_k(x) = (x - x_i)f'_k(x)$  with  $f'_k(x_i) \neq 0$  and apply previous Proposition. Hence for each value of  $i$  such that  $\prod_{j=1}^r a_i^j = 0$ , we should multiply the number in Proposition 6.5 by  $(q - 1)/q$ .  $\square$

Finally, previous corollary with  $l = q$  together with the fact that there are  $\frac{q-1}{2}$  squares in  $\mathbb{F}_q$ , implies the following generalization of Theorem 4.1:

**Theorem 6.7.** *If the degrees  $n_1, \dots, n_{2^r-1}$  go to infinity*

$$\frac{|\{(f_1, \dots, f_{2^r-1}) \in \widehat{\mathcal{F}}_{(n_1, \dots, n_{2^r-1})} : \widehat{S}(f_1, \dots, f_{2^r-1}) = M\}|}{|\widehat{\mathcal{F}}_{(n_1, \dots, n_{2^r-1})}|} = \text{Prob} \left( \sum_{j=1}^{q+1} X_j = M \right)$$

where the  $X_j$  are i.i.d. random variables such that

$$X_i = \begin{cases} -1 & \text{with probability } \frac{(2^r-1)(q+2^r-2)}{2^r(q+2^r-1)} \\ 2^{r-1} - 1 & \text{with probability } \frac{2(2^r-1)}{2^r(q+2^r-1)} \\ 2^r - 1 & \text{with probability } \frac{q}{2^r(q+2^r-1)} \end{cases}.$$

Observe that Theorem 6.7 specializes to Theorem 1.1 of [BDFL09] when  $r = 1$  and to Theorem 4.1 of the present paper when  $r = 2$ .



## APPENDIX

by Alina Bucur.

**1. Biquadratic covers.** Fix a finite field  $\mathbb{F}_q$  of characteristic different from 2. A biquadratic cover of  $\mathbb{P}^1$  over  $\mathbb{F}_q$  is a covering map  $\pi : C \rightarrow \mathbb{P}^1$  such that  $\text{Aut}(C/\mathbb{P}^1) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . Such a cover has an affine model (here we take  $\mathbb{P}^1$  to be marked) given by equations

$$\begin{cases} y_1^2 = h_1(t) \\ y_2^2 = h_2(t) \end{cases}$$

with  $h_1, h_2 \in \mathbb{F}_q[t]$  both square-free. This corresponds to the field extension  $k(\sqrt{h_1}, \sqrt{h_2})$  of the function field  $k = \mathbb{F}_q(t)$  of  $\mathbb{P}^1$ .

Secretly, it also has an implied equation

$$w^2 = h_1(t)h_2(t), \tag{6.1}$$

but of course the right hand side is not necessarily square-free anymore and the gcd of  $h_1$  and  $h_2$  will appear squared. If we denote  $f_3 = \gcd(h_1, h_2)$ , then we can rewrite our three equations as

$$\begin{cases} y_1^2 = f_1(t)f_3(t) \\ y_2^2 = f_2(t)f_3(t) \\ w^2 = f_1(t)f_2(t) \end{cases}$$

with  $f_1, f_2, f_3$  all square-free and pairwise coprime.

This corresponds to the field extension  $K(\sqrt{f_1f_3}, \sqrt{f_2f_3}, \sqrt{f_1f_2})$ . Note that it is better to think of this as a “tri-quadratic” extension, as the roles of  $f_1f_3, f_2f_3, f_1f_2$  can be permuted. This also shows that each cover will appear exactly  $\#S_3 = 6$  times, which is expected as the automorphism group of the Klein group is indeed  $S_3$ .

Let us look at geometric points over a point  $\alpha \in \mathbb{P}^1$ , i.e. we treat our field of definition as algebraically closed.

First, looking at

$$(f_1, f_2, f_3) \bmod (t - \alpha)^2 = (f_1(\alpha) + f_1'(\alpha)(t - \alpha), f_2(\alpha) + f_2'(\alpha)(t - \alpha), f_3(\alpha) + f_3'(\alpha)(t - \alpha)) \bmod (t - \alpha)^2$$

we see that we have:

- $(q^2 - 1)^3$  choices as  $f_1, f_2, f_3$  have to be nonzero  $\bmod (t - \alpha)^2$ .
- from those we need to exclude the possibility that  $(t - \alpha)$  divides any two of  $f_1, f_2, f_3$  (as they have to be coprime), i.e. we cannot allow  $f_1(\alpha), f_2(\alpha), f_3(\alpha)$  to contain two or three zeros. Let us examine each situation we need to avoid.

**Two zeros:** The situation is completely symmetric in  $f_1, f_2, f_3$  so it is enough to count one possibility and multiply by 3. If  $f_1(\alpha) = f_2(\alpha) = 0$ , but  $f_3(\alpha) \neq 0$ , then we must have  $f_1'(\alpha) \neq 0$  (so  $q - 1$  choices),  $f_2'(\alpha) \neq 0$  ( $q - 1$  choices) and no restrictions on  $f_3'(\alpha)$  ( $q$  choices). Taking into account the  $q - 1$  possibilities for  $f_3(\alpha)$ , we have to subtract  $3(q - 1)^3 q$ .

**Three zeros:** In this case we must have  $f_1'(\alpha), f_2'(\alpha), f_3'(\alpha)$  all nonzero, so there are  $(q - 1)^3$  such triples.

Thus we start with

$$(q^2 - 1)^3 - 3q(q - 1)^3 - (q - 1)^3 = q^2(q - 1)^3(q + 3)$$

triples modulo  $(t - \alpha)^2$ .

Geometrically, there are two possibilities for the fiber over  $\alpha$ .

- I.** There will be 4 distinct points when  $f_1(\alpha)f_3(\alpha) \neq 0$  and  $f_2(\alpha)f_3(\alpha) \neq 0$ , i.e. when  $f_1(\alpha), f_2(\alpha), f_3(\alpha)$  are all nonzero ( $(q-1)$  choices each) and  $f'_1(\alpha), f'_2(\alpha), f'_3(\alpha)$  have no restrictions ( $q$  choices each). Thus there are  $q^3(q-1)^3$  possibilities.
- II.** There 2 distinct points otherwise when either  $f_1(\alpha)f_3(\alpha) = 0$  or  $f_2(\alpha)f_3(\alpha) = 0$ . Since no two of the terms can be zero at the same time, this means that exactly one of  $f_1(\alpha), f_2(\alpha), f_3(\alpha)$  is zero. If  $f_1(\alpha) = 0$ , then  $f'_1(\alpha) \neq 0$ . As the situation is again completely symmetric in  $f_1, f_2, f_3$ , we have  $3q^2(q-1)^3$  such triples.

To count  $\mathbb{F}_q$ -rational points, we must split each of the two cases above into two further cases.

- Ia.** The fiber has 4  $\mathbb{F}_q$ -rational points when  $f_1(\alpha)f_3(\alpha)$  and  $f_2(\alpha)f_3(\alpha)$  are both quadratic residues (and non-zero, as we are in the first case above). Thus  $f_1(\alpha), f_2(\alpha), f_3(\alpha)$  have to be all three either quadratic residues or quadratic non residues. In either case they are all nonzero, and thus  $f'_1(\alpha), f'_2(\alpha), f'_3(\alpha)$  have no restrictions imposed on them. Therefore we have

$$2\left(\frac{q-1}{2}\right)^3 q^3 = \frac{q^3(q-1)^3}{4}$$

choices, i.e. probability  $1/4$  to get this subcase out of case I.

- Ib.** There are no rational points (but 2 points of degree 2) in the fiber when exactly one of  $f_1(\alpha), f_2(\alpha), f_3(\alpha)$  is a quadratic residue or exactly one of  $f_1(\alpha), f_2(\alpha), f_3(\alpha)$  is a quadratic nonresidue. This situation occurs with probability  $3/4$  out of case I. (Note that in this case at least one of the two defining equations has no solution, therefore no rational point.)
- IIa.** The fiber consists of 2  $\mathbb{F}_q$ -rational points when one of the following three cases occur.
- $f_1(\alpha)f_3(\alpha) = 0$  and  $f_2(\alpha)f_3(\alpha)$  is a nonzero quadratic residue. Thus we need to have  $f_1(\alpha) = 0, f'_1(\alpha) \neq 0$  and we get

$$2\left(\frac{q-1}{2}\right)^2 (q-1)q^2 = \frac{q^2(q-1)^3}{2} \text{ possibilities.}$$

- $f_2(\alpha)f_3(\alpha) = 0$  and  $f_1(\alpha)f_3(\alpha)$  is a nonzero quadratic residue. As above, there are  $\frac{q^2(q-1)^3}{2}$  such triples.
- $f_3(\alpha) = 0$  and  $f_1(\alpha)f_2(\alpha)$  is a nonzero quadratic residue. Similarly, there are  $\frac{q^2(q-1)^3}{2}$  such triples.

In conclusion, the probability of getting this subcase out of case II is  $1/2$ .

- IIb.** The fiber contains no  $\mathbb{F}_q$ -rational points (it is one double point of degree 2) in one of the following three cases.

- $f_1(\alpha)f_3(\alpha) = 0$  and  $f_2(\alpha)f_3(\alpha)$  is a quadratic nonresidue. There are  $\frac{q^2(q-1)^3}{2}$  such triples.
- $f_1(\alpha)f_3(\alpha)$  is a quadratic nonresidue and  $f_2(\alpha)f_3(\alpha) = 0$ . As before, there are  $\frac{q^2(q-1)^3}{2}$  such triples.
- $f_3(\alpha) = 0$  and  $f_1(\alpha)f_2(\alpha)$  is a quadratic nonresidue. There are also  $\frac{q^2(q-1)^3}{2}$  such triples.

In conclusion, the probability of getting this subcase out of case II is also  $1/2$ .

The upshot is the following “prediction”.

### Conjecture 1.

$$\text{Prob}\left(\#C(\mathbb{F}_q) = M; C \text{ biquadratic cover of } \mathbb{P}^1 \text{ defined over } \mathbb{F}_q\right) \sim \text{Prob}(X_1 + \dots + X_{q+1} = M)$$

where  $X_i$ ’s are i.i.d. random variables taking values

$$X_i = \begin{cases} 4 & \text{with probability } \frac{1}{4} \frac{q^3(q-1)^3}{q^2(q-1)^3(q+3)} = \frac{q}{4(q+3)} \\ 2 & \text{with probability } \frac{1}{2} \frac{3q^2(q-1)^3}{q^2(q-1)^3(q+3)} = \frac{3}{2(q+3)} \\ 0 & \text{with probability } \frac{3q}{4(q+3)} + \frac{3}{2(q+3)} = \frac{3(q+2)}{4(q+3)} \end{cases}$$

Note that the expected number of points in a fiber is 1 and on the whole curve is  $q+1$ .

**2. The general case:  $r$ -quadratic covers.** The argument can be generalized to the case of  $r$ -quadratic covers of  $\mathbb{P}^1$  over  $\mathbb{F}_q$ , i.e. covers  $\pi : C \rightarrow \mathbb{P}^1$  with

$$\text{Aut}(C/\mathbb{P}^1) \simeq \underbrace{\mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}}_{r \text{ times}}.$$

These are precisely the probabilities that appear in Theorem 6.7 of the present paper. Our argument works for any  $r \in \mathbb{Z}_{>0}$ . For  $r = 2$  we will recover the predictions from Section 1. and for  $r = 1$  we will recover the results from [KR09].

An affine model of an  $r$ -quadratic cover is given by equations

$$\begin{cases} y_1^2 = h_1(t) \\ y_2^2 = h_2(t) \\ \vdots \\ y_r^2 = h_r(t), \end{cases}$$

with  $h_1, \dots, h_r \in \mathbb{F}_q[t]$  square-free polynomials. The cover corresponds to the  $r$ -quadratic field extension  $k(\sqrt{h_1}, \sqrt{h_2}, \dots, \sqrt{h_r})$  of  $k = \mathbb{F}_q(t)$ .

Together with the “secret” equations – the equivalents of (6.1) – we get in fact  $2^r - 1$  equations

$$y_J^2 = \prod_{j \in J} h_j(t) \tag{6.2}$$

indexed by the nonempty subsets  $J \subseteq \{1, \dots, r\}$ . Again we want to take out gcd’s as we did in Section 2. We obtain  $f_1, \dots, f_{2^r-1}$  square-free pairwise coprime polynomials that define this extension. (We can do this by choosing any enumeration of the nonempty subsets  $J$ . One possibility is the one described in the proof of Theorem 6.3 in the paper.)

Let us examine the fiber above a point  $\alpha \in \mathbb{P}^1$ . We first consider the geometric points. In order to ease notation, let  $m = 2^r - 1$ . We need to look at

$$(f_1, \dots, f_m) \equiv (f_1(\alpha) + f_1'(\alpha)(t - \alpha), \dots, f_m(\alpha) + f_m'(\alpha)(t - \alpha)) \pmod{(t - \alpha)^2}.$$

First, since

$$(f_1, \dots, f_m) \not\equiv (0, \dots, 0) \pmod{(t - \alpha)^2},$$

we start with at most  $(q^2 - 1)^m$  choices. From these, we need to exclude those that would allow two or more of the  $f_i$ ’s to be divisible by  $(t - \alpha)$ , since they have to be pairwise coprime.

Fix an integer  $k$  with  $1 \leq k \leq m$ . Note that if have exactly  $k$  zeros among  $f_1(\alpha), \dots, f_m(\alpha)$ , then the corresponding derivatives of the  $k$  polynomials that have a zero at  $\alpha$  must be nonzero. Thus, for each choice of  $k$  numbers in  $\{1, \dots, m\}$  we have

$$(q - 1)^k (q - 1)^{m-k} q^{m-k} = q^{m-k} (q - 1)^m \text{ choices.}$$

Therefore we start with

$$(q^2 - 1)^m - \sum_{k=2}^m \binom{m}{k} q^{m-k} (q-1)^m = q^{m-1} (q-1)^m (q+m) \text{ tuples modulo } (t-\alpha)^2.$$

Geometrically, we have the following possibilities.

- I.** There will be  $2^r$  distinct points when  $f_1(\alpha), \dots, f_m(\alpha)$  are all nonzero. Again in this case we have no restrictions on the derivatives. Thus we have  $(q-1)^m q^m$  possibilities.
- II.** Otherwise, only one of the  $f_1(\alpha), \dots, f_m(\alpha)$  can be zero (as the  $f_j$ s are pairwise coprime). In this case, the fiber will contain  $2^{r-1}$  geometric points. The situation is completely symmetric in  $f_1, \dots, f_m$ . Thus, it is enough to count the case when  $f_1(\alpha) = 0$  and multiply the result by  $m$ . Then  $f'_1(\alpha) \neq 0$  so the derivative can take  $(q-1)$  values. For the other  $m-1$  terms, we have  $f_j(\alpha) \neq 0$ , so it can take  $(q-1)$  values, and there are no restrictions on the derivatives  $f'_j(\alpha)$ ,  $2 \leq j \leq m$ . This means that there are  $m(q-1)(q-1)^{m-1} q^m$  choices in total that lead to this case. Note that this is equal to

$$mq^{m-1}(q-1)^m = q^{m-1}(q-1)^m(q+m) - q^m(q-1)^m.$$

We now look at the  $\mathbb{F}_q$ -rational points in the fiber above  $\alpha$ . The two cases above split into two cases each.

- Ia.** The fiber has  $2^r$   $\mathbb{F}_q$ -rational points which occurs with probability  $1/2^r$  out of case I.
- Ib.** The fiber has no  $\mathbb{F}_q$ -rational points which occurs with probability  $(2^r - 1)/2^r$  out of case I.
- IIa.** The fiber consists of  $2^{r-1}$   $\mathbb{F}_q$ -rational points which occurs with probability  $1/2^{r-1}$  out of case II.
- IIb.** The fiber contains no  $\mathbb{F}_q$ -rational points which occurs with probability  $(2^{r-1} - 1)/2^{r-1}$  out of case II.

Note that this already tells us that the expected number of points in a fiber is 1 and on the whole curve is  $q+1$ . Another interesting observation is that the case of biquadratic extensions is a bit different than the general case. For instance, for  $r=2$  case II splits into two subcases with probability 50-50; but in general the probabilities for the subcases IIa and IIb are  $2^{1-r}$  and  $(1-2^{1-r})$ . Which means that one has to look at the case  $r \geq 3$  in order to get the complete picture.

Since  $m = 2^r - 1$  we get the following prediction.

## Conjecture 2.

$$\text{Prob}(\#C(\mathbb{F}_q) = M; C \text{ } r\text{-quadratic cover of } \mathbb{P}^1 \text{ defined over } \mathbb{F}_q) \sim \text{Prob}(X_1 + \dots + X_{q+1} = M)$$

where  $X_i$ 's are i.i.d. random variables taking values

$$X_i = \begin{cases} 2^r & \text{with probability } \frac{1}{2^r} \cdot \frac{q^m (q-1)^m}{q^{m-1} (q-1)^m (q+m)} = \frac{q}{2^r (q+m)} = \frac{q}{2^r (q+2^r-1)} \\ 2^{r-1} & \text{with probability } \frac{1}{2^{r-1}} \cdot \frac{mq^{m-1} (q-1)^m}{q^{m-1} (q-1)^m (q+m)} = \frac{m}{2^{r-1} (q+m)} = \frac{2^r-1}{2^{r-1} (q+2^r-1)} \\ 0 & \text{with probability } \frac{(2^r-1)(q+2^r-2)}{2^r (q+2^r-1)}. \end{cases}$$

These are exactly the probabilities that appear in Theorem 6.7 of the present paper.

The argument works for any  $r \in \mathbb{Z}_{>0}$ . For  $r=2$  we recover the predictions from previous Section; for  $r=1$  we recover the random variables from [KR09].

## REFERENCES

- [BDFL09] A. Bucur, C. David, B. Feigon, M. Lálín, *Statistics for traces of cyclic trigonal curves over finite fields*, Int. Math. Res. Not. (2009), 932–967.
  - [BDFL11] A. Bucur, C. David, B. Feigon, M. Lálín, *Biased statistics for traces of cyclic  $p$ -fold covers over finite fields*, WIN - Women in Number, Fields Institute Communications, American Mathematical Society (2011).
  - [BDF<sup>+</sup>15] A. Bucur, C. David, B. Feigon, N. Kaplan, M. Lálín, E. Ozman, M. Wood, *The distribution of  $\mathbb{F}_q$ -points on cyclic  $\ell$ -covers of genus  $g$*  (2015). Available at arXiv: 1505.07136.
  - [Bil95] P. Billingsley, *Probability and measure*, Wiley Series in Probability and Mathematical Statistics, New York: John Wiley, 1995.
  - [DS94] P. Diaconis, M. Shahshahani, *On the eigenvalues of random matrices*, J. Appl. Probab. **31A** (1994), 49–62.
  - [GP05a] D. Glass, R. Pries, *Hyperelliptic curves with prescribed  $p$ -torsion*, Manuscripta **117** (2005), no. 3, 299–317.
  - [GP05b] D. Glass, R. Pries, *On the moduli space of Klein four covers of the projective line*, Computational Aspects of Algebraic Curves, ed. T. Shaska, Lecture Notes Series in Computing **13**, 2005.
  - [GGL95] R. L. Graham, M. Grötschel, L. Lovász, *Handbook of combinatorics, Volume 2*, Elsevier Science, 1995.
  - [Har77] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics vol. 52, Springer-Verlag, New York, 1977.
  - [KR09] P. Kurlberg, Z. Rudnick, *The fluctuation in the number of points on a hyperelliptic curve over a finite field*, J. Number Theory **129** (2009), no. 3, 580–587.
  - [KS99] N. M. Katz, P. Sarnak, *Random matrices, Frobenius eigenvalues and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999.
  - [LS96] H. W. Lenstra, P. Stevenhagen, *Chebotarëv and his density theorem*, The Mathematical Intelligencer **18** (1996), 26–37.
  - [Ros02] M. Rosen, *Number theory in function fields*, XI, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.
  - [Woo12] M. Wood, *The distribution of the number of points on trigonal curves over  $\mathbb{F}_q$* , Int. Math. Res. Not. (2012), no. 23, 5444–5456.
  - [Xio10] M. Xiong, *The fluctuations in the number of points on a family of curves over a finite field*, Journal de Théorie de Nombres de Bordeaux **3** (2010), 755–769.
- UNIVERSITEIT LEIDEN, MATHEMATISCH INSTITUUT, NIELS BOHRWEG 1, 2333 CA LEIDEN (THE NETHERLANDS)  
*E-mail address:* `e.lorenzo.garcia@math.leidenuniv.nl`
- UNIVERSITÀ DEGLI STUDI “ROMA TRE”, DIPARTIMENTO DI MATEMATICA E FISICA, LARGO SAN LEONARDO MURIALDO 1, 00146 ROMA (ITALY)  
*E-mail address:* `meleleo@mat.uniroma3.it`
- UNIVERSITAT DE BARCELONA, DEPARTAMENT D’ÀLGEBRA I GEOMETRIA, GRAN VIA DE LES CORTS CATALANES 585, 08005 BARCELONA (SPAIN)  
*E-mail address:* `pmilione@ub.edu`
- UNIVERSITY OF CALIFORNIA, SAN DIEGO, DEPARTMENT OF MATHEMATICS, 9500 GILMAN DRIVE #0112, CA 92093 LA JOLLA (USA)  
*E-mail address:* `alina@math.ucsd.edu`